KEEPER | Pressemitteilung

Keeper Security stellt KeeperAI zur Erkennung und Abwehr von Cyberbedrohungen in Echtzeit vor

Die agentenbasierte KI-Lösung von Keeper überwacht und analysiert privilegierte Sitzungen, um Angriffe sofort zu erkennen und zu beenden.

München, 27. August 2025 – Da Cyberangriffe immer schneller, umfassender und zunehmend automatisiert unter Verwendung von künstlicher Intelligenz erfolgen, haben Unternehmen Schwierigkeiten, mit den modernen Bedrohungen Schritt zu halten. Privilegierte Konten, die Zugriff auf die sensibelsten Systeme innerhalb eines Unternehmens gewähren, bleiben weiterhin die Hauptziele. Doch herkömmliche Sicherheitstools erkennen komplexe Insider-Bedrohungen und Anomalien auf Sitzungsebene oft erst dann, wenn eine Sicherheitsverletzung bereits stattgefunden hat.

Heute kündigt Keeper Security, ein führender Anbieter von Zero-Trust- und Zero-Knowledge-Software für privilegierten Zugriff (PAM) zum Schutz von Passwörtern und Passkeys, privilegierten Konten, Geheimnissen und Remote-Verbindungen, KeeperAI an. KeeperAI ist die neue, anpassbare und agentenbasierte KI-Funktion für die KeeperPAM®-Plattform und ermöglicht die Überwachung und Analyse von Sitzungen in Echtzeit, die automatisierte Klassifizierung von Bedrohungen und die sofortige Reaktion zur Bekämpfung von Cyberangriffen und verdächtigem Verhalten.

„In der Realität stellt sich nicht die Frage, ob Cyberbedrohungen stattfinden, sondern wann und wie schnell Unternehmen reagieren“, sagt Craig Lurey, CTO und Mitbegründer von Keeper Security. „Mit den agentenbasierten Funktionen von KeeperAI können Unternehmen Bedrohungen automatisch in Echtzeit überwachen, identifizieren und abwehren und so risikoreiche Sitzungen, unbefugte Zugriffe oder unzulässige Kontoerweiterungen unterbinden.“

Bewältigung heutiger Sicherheitsherausforderungen

Insider-Bedrohungen, Missbrauch von Berechtigungen und fortgeschrittene persistente Bedrohungen (Advanced Persistant Threats) stellen Sicherheitsteams seit langem vor Herausforderungen. In Zeiten KI-gestützter Cyberangriffe können traditionelle manuelle Sitzungsüberprüfungen und regelbasierte Warnmeldungen mit den sich schnell entwickelnden Bedrohungen nicht mehr Schritt halten. KeeperAI begegnet dieser Herausforderung mit einer kontinuierlichen Überwachung privilegierter Sitzungen, einer automatischen Risikoklassifizierung und Sitzungszusammenfassungen. Es unterstützt mit konfigurierbaren Reaktionen, die Sitzungen beenden oder Warnmeldungen auslösen, wenn ein verdächtiges und böswilliges Verhalten erkannt wird – ohne dass ein menschliches Eingreifen erforderlich ist. Als souveränes KI-Produkt hat jedes Unternehmen, mit KeeperAI die vollen Eigentums- und Kontrollrechte über seine verwendeten oder generierten Daten.

Zu den wichtigsten Funktionen von KeeperAI gehören:

- **Automatisierte Sitzungsanalyse**: Analyse von Sitzungsmetadaten, Tastenanschlagprotokollen und Befehlsausführungsprotokollen zur Erkennung ungewöhnlicher Verhaltensweisen.

- **Bedrohungsklassifizierung**: Automatische Kategorisierung erkannter Bedrohungen und Zuweisung von Risikostufen.
- **Sitzungsterminierung**: Auslösen einer automatischen Sitzungsterminierung auf der Grundlage der festgelegten Bedrohungsklassifizierung.
- **Anpassbare Konfiguration**: Anpassung der Risikoparameter und Erkennungsregeln an die Umgebung des Unternehmens.
- **Sitzungssuche**: Durchsuchen von Sitzungen, um bestimmte Schlüsselwörter oder Aktivitäten zu finden.
- **Flexible Bereitstellung**: Unterstützung für LLM-Inferenz von Drittanbietern, cloudbasiert und on-premises.

KeeperAI kategorisiert Befehle in Bedrohungsrisikostufen von „kritisch“ über „hoch“ und „mittel“ bis „niedrig“. Sobald KeeperAI aktiviert ist, können Administratoren die Risikostufenklassifizierung und die Erkennungsrichtlinien anpassen und damit regelbasierte Richtlinien für bestimmte Befehlsmuster definieren – mit der Option, riskante Sitzungen automatisch zu beenden oder sie einfach zu überwachen, wenn Bedrohungen erkannt werden. Die Lösung ermöglicht Kunden die Integration mit großen LLM-Anbietern wie AWS Bedrock, Anthropic, Google Gemini und OpenAI. Sie unterstützt kompatible Cloud- und lokale Bereitstellungen ohne Herstellerabhängigkeit.

„Sicherheitsteams sollten keine Stunden damit verschwenden müssen, Protokolle zu überprüfen oder riskante Sitzungen manuell zu beenden“, sagt Jeremy London, Director of Engineering, AI and Threat Analytics bei Keeper Security. „Aus diesem Grund haben wir KeeperAI als agentenbasiertes KI-System entwickelt. Es erkennt nicht nur Anomalien, sondern überwacht diese aktiv und ergreift in Echtzeit Maßnahmen. Mit von Menschen konfigurierten Kontrollen und Parametern beendet KeeperAI selbstständig risikoreiche Sitzungen und setzt Sicherheitsrichtlinien sofort durch. Dies unterbindet Alarmmüdigkeit, beschleunigt die Reaktionszeiten auf Sekunden und ermöglicht es den Teams, sich auf die Strategie zu konzentrieren, anstatt nur Brände zu löschen.“

Entwickelt für spürbare Wirkung
KeeperAI unterstützt derzeit SSH-basierte Sitzungen. Eine Erweiterung der Unterstützung auf RDP, VNC, RBI und Datenbankprotokolle ist geplant. Alle Risikobewertungen und Vorfalldaten werden direkt in die Keeper Vault-Benutzeroberfläche eingespeist, sodass Sicherheits-Teams Vorfälle untersuchen, die Compliance aufrechterhalten und über das Advanced Reporting and Alerts Module (ARAM) von Keeper eine Integration mit SIEM- (Security Information and Event Management) und SOC-Tools (Security Operations Center) vornehmen können.

Die Lösung kombiniert agentenbasierte KI mit einer Zero-Knowledge-Architektur, sodass alle sensiblen Daten verschlüsselt und unter der Kontrolle des Kunden bleiben. Unternehmen profitieren von skalierbaren Sicherheitsmaßnahmen und erfüllen gleichzeitig die Compliance-Anforderungen.

Verfügbarkeit
KeeperAI ist ab sofort für alle KeeperPAM-Kunden verfügbar, die PAM Gateway Version 1.7.0 oder höher verwenden, und kann sowohl in Cloud- als auch in Docker-basierten Umgebungen eingesetzt werden. Weitere Informationen oder zur Aktivierung von KeeperAI stehen in der Keeper-Dokumentation.

###

Über Keeper Security:
Keeper Security verändert die Cybersicherheit für Millionen von Einzelpersonen und Tausende von Unternehmen weltweit. Die intuitive Cybersicherheitsplattform von Keeper ist mit einer End-to-End-Verschlüsselung ausgestattet und genießt das Vertrauen von Fortune-100-Unternehmen, um jeden Benutzer auf jedem Gerät und an jedem Standort zu schützen. Unsere patentierte Zero-Trust- und Zero-Knowledge-Lösung für das Privileged Access Management vereint die Verwaltung von Unternehmenspasswörtern, Geheimnissen und Verbindungen mit Zero-Trust-Netzwerkzugriffen und Remote-Browser-Isolation. Durch die Kombination dieser wichtigen Identitäts- und Zugriffsverwaltungskomponenten in einer einzigen cloudbasierten Lösung bietet Keeper beispiellose Transparenz, Sicherheit und Kontrolle und gewährleistet gleichzeitig die Einhaltung von Compliance- und Audit-Anforderungen. Erfahren Sie unter KeeperSecurity.com, wie Keeper Ihr Unternehmen vor den heutigen Cyberbedrohungen schützen kann.

Folgen Sie Keeper auf Facebook Instagram LinkedIn X YouTube TikTok

Pressekontakt für Keeper in DACH:
Alexandra Schmidt, +49 170 387 10 64
Thilo Christ, +49 171 622 06 10
keeper@tc-communications.de